

references were properly combinable, they teach away from Applicants' claimed invention.

The Office Action appears to mischaracterize the claim language by stating that the claims are directed to apparatus and methods that give users the ability to define the validity period for certificates. This is not the case. To the contrary, Applicants claim a completely different system. For example, as set forth in Claim 1, Applicants claim, inter alia, providing, through a multi-client manager unit, selectable digital signature expiry data including at least public verification key expiry data, and selectable private signing key expiry data, that are selectable on a per client basis wherein the digital signature key pairs are not shared among users. As such, a certification authority, or other trusted authority, has the ability to selectably vary public key verification expiry data and private signing key expiry data on a per client basis. Such a system offers many advantages over the prior art, including, but not limited to, a trusted system wherein the user cannot act as a trust authority and effectively override the entire trust relationships of the system.

For example, Ellison teaches giving the users the ability to define the validity period for certificates. This teaching effectively allows a user to override any trust given by a certification authority. By way of example, Ellison apparently teaches that a user may decide that they want a ten year validity period for carrying out bank transactions. Such a system would not be very useful since a certification authority would have no control over user trust periods. In contrast, Applicants claim a multi-client trust authority wherein the user does not, on its own, have the ability to define the validity period of certificates. Instead, the validity periods are selectable on a per client basis through a trust authority so that differing clients may have differing validity periods for their various keys. The users are not selecting the validity periods. Accordingly, Applicants respectfully submit that the claims are in condition for allowance.

In addition, Ellison also is silent as to how to obtain new keys in such a system and how such a system would actually function.

Moreover, Applicants respectfully submit that the teachings of Lewis cannot be cited without consideration of how the Lewis invention carries out its disclosed process. The Lewis reference is directed to a key replacement system in a public key cryptosystem. The Lewis system does not teach or suggest, inter alia, selectably varying key expiry data for digital signatures or encryption keys as claimed. In fact, Lewis is directed to a completely different problem. The Lewis reference is directed to selecting replacement keys so that it is computationally difficult to determine a replacement key from its masked version. An active public key and a hash of a replacement key is provided by a key server to nodes of the network. Each time a key request is performed, the active public key is discarded. A key replacement message is signed by an active private key and a replacement private key. Accordingly, the message is signed by a replacement private key from an entity that knows the replacement private key before the message is sent. In addition, cited sections of Ellison appear to be silent as to any suitable key replacement mechanism. Accordingly, the references are not properly combinable.

Applicants also submit that the dependent claims add additional novel subject matter. For example, Claim 2 requires, inter alia, that the selectable expiry data is digital signature certificate lifetime data for variably setting a lifetime end date for a digital signature associated with a given client. Ellison has been cited as teaching such information. However, as noted above, Ellison teaches away from the claimed invention and does not indicate that the selectable expiry data is provided through a multi-client manager unit or that the data is selectable on a per client basis. In fact, Ellison teaches a distinctly differently system. Accordingly, this claim is believed allowable.

As to Claim 3, the Office Action cites Col. 7, lines 64-65 of the Lewis reference. This portion of Lewis merely states that the key service sends a key replacement message to each node or broadcasts a single key replacement message. There is no mention of privilege control. The claimed method includes, inter alia, providing variable update privilege control on a per client basis to facilitate denial of updating the digital signature key pair on a per client basis. Applicants respectfully request the teaching of such a privilege control mechanism as claimed.

As to Claim 4, the Office Action appears to be silent as to a rejection of this claim. Applicants respectfully submit that this claim adds additional patentable subject matter and is also allowable.

As to Claim 6, the Office Action indicates that it is inherent in Ellison. Applicants respectfully reassert the remarks made with respect to Ellison and note that Ellison is silent as to a multi-client manager unit having, inter alia, a user interface that facilitates setting of a selectable expiry data on a per client basis to a desired date. Accordingly, Applicants respectfully submit that this claim is also in condition for allowance.

As to Claim 8, the Office Action appears to be silent as to a rejection for this claim. Applicants respectfully submit that this claim adds additional patentable subject matter and is condition for allowance.

As to Claim 9, the Office Action indicates that the limitations of Claim 9 are anticipated by Lewis. Applicants respectfully reassert the remarks made above with respect to Lewis and further note that the Office Action admits that Lewis does not teach, inter alia, providing, through a client manager unit, selectable expiry data that is selectable on a per client basis.

As to Claims 10-18, the Office Action appears to be silent as to rejections for these claims. Applicants respectfully submit that these claims add additional patentable subject matter and are also in condition for allowance.

As to Claims 20, 24 and 26, the Office Action appears to be silent as to rejections for these claims. Applicants respectfully submit that these claims add additional patentable subject matter and are also in condition for allowance.

Claims 5, 19 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis and Ellison as applied to Claims 1, 14 and 21 and further in view of Applicants' admitted prior art. Applicants respectfully reassert the remarks made above with respect to Claims 1, 14 and 21.

The Office Action takes official note that fixed length renewal periods are old and well known. The Office Action then concludes that it would have been obvious to set key update periods that are based on a fixed number of days and a percentage of a key's lifetime. Applicants respectfully submit that this is a mischaracterization of Applicants' claimed invention. Applicants note that conventional public key cryptographic systems typically have a fixed default period that is the same for all clients on the system. The default period is fixed and it is typically not adjustable by a multi-client manager or certification authority as claimed. However, Applicants claim, inter alia, initiating, by a client unit, digital signature key pair update requests based on whether differences between a current date and a digital signature private key lifetime end date is less than an absolute predetermined period of time, and based on whether the difference between a current date and a digital signature private key lifetime end date is less than a predetermined percentage of a total duration of a digital signature private key lifetime when the digital signature private key lifetime was selectable on a per client basis through a multi-client manager unit. No such digital key pair update request or basis for such a request is taught or suggested in any of the references cited. It is Applicants' own

disclosure which teaches such an invention which provides many advantages over conventional systems. Applicants respectfully request a showing of a teaching and references of such a digital signature key pair update request and the basis for initiating such a request as claimed.


Claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis and Ellison as applied to Claim 1 above. Applicants respectfully reassert the remarks made above with respect to Claim 1 and also respectfully submit that Lewis does not teach or suggest, inter alia, generating, by the multi-client manager unit, the new digital signature key pair for a client in response to the multi-client manager unit receiving a digital signature key pair update request. Applicants respectfully request a showing of such a teaching.

Applicants believe that the claims are in condition for allowance and that the dependent claims add additional novel subject matter. The Examiner is invited to contact the undersigned attorney by telephone or facsimile if the Examiner believes that such a communication would advance the prosecution of the present patent application.

Respectfully submitted,

MARKISON & RECKAMP, P.C.

By

  
Christopher J. Reckamp  
Registration No 34,414

Date: September 7, 2000

MARKISON & RECKAMP, P.C.  
P.O. Box 06229, Wacker Drive  
Chicago, IL 60606-0229  
(312) 939-9800  
FAX: (312) 939-9828